Volume 18, Issue 45   Atari Online News, Etc.   December 2, 2016

Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1845   12/02/16

~ Facebook Admits "Wrong" ~ Avalanche Taken Down! ~ Facebook in China?

-* Call for Firebee Donations! *-
-* Video Game Buying Guide for 2016! *-
-* Thea Realm Fighters for Jaguar Discovered! *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""

Well, we missed our post-Thanksgiving issue due to a vast shortage of material - sorry. A belated Thanksgiving greetings’ we all hope that your holiday was a good one. My only regret is that my turkey leftovers didn’t last as long as usual! Next year, I’ll have to plan a little bit better!

It’s hard to believe that we’re already into the month of December! No snow on the ground, fortunately! I’m not ready for a New England winter, but then again, I rarely am. I’m not looking forward to having to deal with the cold and snow; I’m hoping that we can experience a mild season similar to what we had last year.

We’re still dealing with post-election issues, but not surprisingly. As President-elect Trump moves forward trying to get his Cabinet put together, we’re still facing a variety of backlash from anti-Trump factions. This, in my opinion, is going to continue for quite some time.

Until next time...

=~=~=~=

ARAnyM MiniPack

Hi,

ARAnyM <http://aranym.org/> is the GNU/GPL ATARI Virtual Machine from which a minimal configuration, the *miniPack* is distributed <http://eureka.atari.org/miniPack.zip> miniPack is modified with the new release of TeraDesk v.4.0.7. It supports:

- hide quoted text -
‘Run_win‘ allows launching on PC with Windows
‘MacAranym‘ allows launching on PPC Macintosh with OS X
‘MacAranym JIT‘ allows launching on IntelMac with OS X
‘run_x86.sh‘ allows launching on PC with x86-Linux
‘run_ppc.sh‘ allows launching on Mac _and_ PS3 with PPC-Linux

So Macintosh-PC-PlayStation3 are all supported with Windows, OS X and GNU/Linux.

This simple ARAnyM configuration is running on any machine. Here is a screenshot at <http://eureka.atari.org/aranym.gif>

Enjoy, it’s yours =)

--
François LE COAT
Author of Eureka 2.12 (2D Graph Describer, 3D Modeller)
<http://eureka.atari.org/>

TeraDesk 4.07

2016-11-30:

A new version of the TeraDesk desktop is available.

The new 4.07 is mainly a bug fix version with only a minor new feature: the option to change TeraDesk’s behaviour when opening links to directories (Additional details are available in TeraDesk’s documents).

The new version of TeraDesk can be downloaded at: tera407.zip

As there were no changes in the resource files from version 4.06 to 4.07, old RSC files can still be used. Russian Teradesk 4.07, with up-to-date documents is already available, while other 4.07 will follow soon. As before, Nationalized version of TeraDesk are available at the Kurobox ftp server:
ftp://kurobox.serveftp.net:30 ... /desktops/

EmuTOS 0.9.7

2016-11-23

A new version of our Open-Source Operating System is available.

As we already announced on the mailing list, a new version of the alternative Open-Source operating system for Atari platforms has recently been released. EmuTOS will continue to be improved, and the team around Roger Burrows has once again done a great job. Besides the "small bugfixes" there are 58 new functions and larger fixes in this new release! FireBee owners will directly benefit from many of these improvements. Some good examples would be the new, extended MBR partitions or the independently runnable version of EmuCON2.

As always, EmuTOS will be flashed into the ROM of the FireBee with flash_cf.prg, and can then either be used as the completely independent standard OS by selecting it through the DIP-switches; or by selecting it in the boot menu of FireTOS (then it can also use the USB-drivers of FireTOS).

EmuTOS is a pure ColdFire operating system, so it will harness the full power of the V4e processor. This is especially interesting for a ColdFire FreeMiNT multitasking system - the combination preferred by most "Unixophile" FireBee open-source users and developers.

The package "emutos-firebee-0.9.7.zip" with the new operating system can be downloaded from the SourceForge pages of the project.

Delivery and Call for Donations

Dear Atari-Community. The delivery of the second Firebee-series has finally begun.

Since we currently are receiving the modified boards in small batches from the assembly company as announced before, the computers will be sent out in the order they were ordered. Thank you once again for your patience. The computers will have, as had been mentioned several times, two years of warranty.

We now also know the exact costs for the whole "game" with the busdriver-components. All in all, Medusa Computer Systems now has to pay 2720.- Euros extra for searching the cause of the problem and for refitting the boards. Since we calculated the prices very narrowly in order to be able to pass on the 40.- Euro price reduction to you, we don’t want to just increase the fixed price again now. Instead, we will try an experiment. We would like to collect the 2720.- Euro in a solidary effort. Anyone who can afford it could pay a little more, those who are short on money only a very small amount. Maybe there are also people that have not (yet) ordererd a computer and still would like to support the project. Therefore we would like to ask you to pool up and provide the money together. Everything that won’t come in through you will have to be paid by MCS itself...

All donations can be sent to the SEPA bank account of MCS or via Paypal.

MCS Aschwanden
Buchhaldenstr.16
8610 Uster
Switzerland
Bank account Nr.: 202-805498.40F
IBAN: CH22 0020 2202 8054 9840 F
BIC: UBSWCHZH80A
"reason for payment": FB series 2 donation

=~=~=~=

->In This Week’s Gaming Section - All You Need To Know About Final Fantasy XV!

""""""""""""""""""""""""""""" Video Game Buying Guide 2016!
Atari Jaguar Game Thea Realm Fighters Discovered, Released

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Everything You Need To Know About Final Fantasy XV

Final Fantasy XV has been a massive undertaking for years now, but it’s finally on the horizon!

The last full-length main Final Fantasy game launched way back in 2009 with Final Fantasy XIII. Final Fantasy XV has been in development for nearly ten years, which has left fans with a lot of questions about the game. That’s why we’re here.

We’ve put together this guide full of the things you ought to know before you dive into the meat of the game. We’ll cover the battle system, the world of Eos, the characters, and more!

Final Fantasy XV takes place in the world of Eos. To put it bluntly, this world is absolutely massive. It has been predicted that the main continent roughly scales to 780 square miles and several times the magnitude of the main continent from The Witcher 3. It’s also much, much larger than Grand Theft Auto V. This means that Final Fantasy XV may be one of the largest open world games released in recent times.

While there is a main quest, and story to follow, you have much more freedom in Final Fantasy XV than we’ve ever seen. In the past, the open world didn’t crop up until you were hours and hours into the game. That isn’t the case here. Since you’re on a road trip, you are given the chance to start exploring the world within the first ten minutes.

There are also multiple continents on Eos. Each one has it’s own weather patterns, so you can expect to run into storms, snow, sunny days and more.

There are also several different kinds of transportation that are available in Final Fantasy XV. Your main mode of travel is the car that Noctis and his friends all ride around in, The Regalia. The Regalia is a pretty sweet ride, with some hidden features but it’s far from the only way you can move around. There is of course always running around on foot, along with the return of a franchise favorite; Chocobos.

The Regalia is one of the stars of the show, though. It’s a convertible that can switch between a hard top and no roof depending on the weather. Since the game is based around a road trip, the Regalia is a consistent part of this. You’ll spend a good chunk of your time driving along scenic roads, and you will need to stop to camp for the evening, or to refuel your car at gas stations. The Regalia isn’t just a car, though, later on in the game, it is actually able to fly.

Final Fantasy XV revolves around Noctis, the Prince of Lucis and his three friends. After years of cold war between Lucis and the Empire Niflheim over the last remaining crystal of power, a peace accord has been reached. As part of the agreement, Noctis is to wed Lady Lunafreya of the imperial province of Tenebrae in the city of Altissia.

Before the treaty can be signed, Noctis along with Gladiolus, Ignis, and Prompto head for the site of the wedding. Before they get very far, though, news reaches them. The Niflheim Empire used the peace treaty as a guise and invaded Lucis, destroying the capital city of Insomnia.

Reports that King Regis, Luna and Noctis himself have been killed reach the party, along with the fact that the Lucian Crystal has been stolen. Rather than fall to despair, Noctis and his friends start a quest. They’ll have to outrun Niflheim, somehow recapture the Lucian Crystal, and reclaim the Throne.

The Characters

Unlike earlier games that had a fairly large spread of playable characters in your party, there are four in Final Fantasy XV. Noctis, Prompto, Ignis and Gladiolus. Each one has their one perks and drawbacks, and each one adds to the story in different ways.

Noctis is the main character, and he is the Prince of Lucis. This is the guy that the whole story revolves around. One of his most exciting abilities is used in battle, Warp Strike. Using this ability Noctis can throw his sword and then teleport to wherever it lands on the field of battle. Warp Strike makes it easy to get out of the way of a nasty hit, or to get closer to the action in question.

Gladiolus Amicitia is Noctis’s bodyguard. The eldest son of a noble family that serves the royal family, Gladiolus takes his position pretty seriously. However, his relationship with Noctis is more like a brother than an aloof bodyguard.

Ignis Scientia has been raised alongside Noctis since they were children. His role in life is to act as an advisor to Noctis. He’s a somewhat reserved, but highly intelligent young man. A tactical mind, he is the one who cooks for our party when you stop to make camp on your journey.

Prompto Argentum has been Noctis’s friend since high school, but he is not from a high-born family. Instead of being bound by duty, he is here because he is loyal to Noctis. He’s also the comedic relief our of the group, trying to lift everyone’s spirit. While Prompto is the weakest member of the time physically, he can chain attacks with Noctis making him much nastier against enemies.

There is also the Lady Lunafreya Nox Fleuret, the childhood friend, and now fiancee of Noctis. Luna is a captive of the Niflheim Empire but is still the youngest Oracle in history. Her ability to speak to the Gods has given her country of Tenebrae a degree of autonomy they would not otherwise have. She and Noctis have a long, and complicated history, and she is the main heroine in Final Fantasy XV.

One of the core facets of Final Fantasy games has long been it’s combat system. In each game, we see a slightly different system that has adapted to the way gaming has evolved over time. The system in Final Fantasy XV is no different, and they have made serious strides. The aim is to deliver a seamless action RPG experience that allows you a degree of customization in how you play.

You receive four slots to equip weapons, magic or shields. However, you only control Noctis in combat. You can still chain combos with other members of the team, and combat is entirely active time. There is no waiting for your turn to attack, and using Warp Strike you can move quickly and efficiently in and through the battle. Hitting L1 and a direction on the D-pad will let you call your friends to you, make strategic strikes easy and effective as well.

It wouldn’t be a Final Fantasy game without magic, right? You’ll find both summons   known as Astrals   and magic in Final Fantasy XV. Magic is found in the environment around you, and while there are only four basic types, you can customize things to your liking. You’ll need to draw the magic, and then transfer it into a flask before use.

When you go to put magic into a flask, you can put two kinds of magic into it. You can also use items to customize your magic further, letting you fine tune it to do as much damage as possible. There is a second magic type beyond the elemental kind, but there aren’t many details on it quite yet.

There is a ton more to see, and then hundreds of things to do within the game. Multiple mini-games, side quests, and places for you to explore when Final Fantasy XV releases on November 29th, 2016. This is just the very surface of things. You can expect plenty more from us about Final Fantasy XV as well. Our review is coming next week, followed by all the content you need for your adventures in Eos.

Video Game Buying Guide 2016

Black Friday and Cyber Monday are fast approaching, and that means tons of great deals on video games and systems. But which should you buy first? Start with these.

NES Classic Edition
($60)

It s been awhile since Nintendo could claim to have the hottest holiday tech toy, but make no mistake: gamers are going nuts for the NES Classic Edition. Sold out within hours of going on sale, this adorable, pint-sized replica of Nintendo s beloved home console plugs right into your TV to deliver 30 awesome NES games. It even includes a spot-on version of the NES controller, and while the cords are all too short, the gaming goodness packed in this glorious stocking stuffer will last many, many months. It ll be tough to find, but it s worth the effort.

Dishonored 2
($60 | PS4, Xbox One, PC)

Let the elf keep an eye on the kids while you enjoy a little stealth on the shelf this year. The sequel to 2012 s Game of the Year, Dishonored 2 ups the ante with two unique playable characters thrust into a stunning steampunk world brimming with danger and choice. Do you sneak through windows and pounce on unknowing bad guys, or wreak havoc with potent mystical powers? Either way, you can t go wrong.

Overwatch
($60 | PS4, Xbox One, PC)

Blizzard Entertainment has made a fortune off this beautifully polished and brilliantly balanced online shooter, but if you or someone you love isn t among the 20 million who have already bought Overwatch, don t hesitate to join the crew. On the fast track to becoming The Next Big Thing in competitive gaming, Overwatch is also a ton of fun with a group of friends. Just don t main Bastion. Seriously.

PokØmon Sun/Moon
($50 | 3DS)

Finally stopped playing PokØmon Go? Good. Now put down your smartphone and pick up a 3DS: you re ready for a real PokØmon game. Commemorating 20 years of PokØmon, Sun/Moon takes place in a new tropical setting yielding plenty of new pokØmon and features. Long time fans will dig refinements like an upgraded PokØdex and the ability to refresh your pokØmon after battle. Addictive and colorful, it s another time-sucking treat from the masters of the craft.

Skylanders: Imaginators
($75 | PS3, PS4, Xbox 360, Xbox One, Wii U)

While fellow toys-to-life franchise Disney Infinity closed shop this year, Skylanders keeps right on ticking. The latest offers a cool twist that kids young and old alike will love: the ability to create their own Skylander, customize it, and even order a 3D printed version. It s still a bit devious with how it locks out content, though, so be prepared to cough up more dough on extra toys as we roll into the new year. (Starter Pack: $75 for PS4, Xbox One | $65 for Xbox 360, PS3, Wii U)

Civilization VI
($60 | PC)

Just one more turn, they say, but they really mean, just 36 more turns and okay maybe 10 more after that. The most addictive strategy game ever returns in its sixth incarnation, and it s one of the best yet. Richly complex yet still surprisingly accessible, it retains its core gameplay but introduces cool new features like unstacked cities and a Civics tech tree. The result breathes life into the 25-year-old formula, still the perfect gift for the PC gamer in your life.

Battlefield 1
($60 | PS4, Xbox One, PC)

While Call of Duty forges into the future, EA s Battlefield series smartly took a step back into history by tackling World War I. It was a great choice; this is one of the best Battlefield games in ages, bringing the franchise s brilliantly chaotic multiplayer to a gripping old-school arena. It also rectifies a longstanding critique of Battlefield by including a genuinely moving single-player campaign. Enlist today.

Forza Horizon 3
($39 | Xbox One, PC)

There are a great many reasons to own an Xbox One, but this season, there is one really, really great one: Forza Horizon 3. Explore a wide-open virtual Australia from behind the wheel of vehicles both exotic and mundane. Whether you re smashing through the outback or needling through tight streets, you ll marvel at the drop-dead gorgeous graphics and perfect handling.

NBA 2K17
($60 | PS3, PS4, Xbox 360, Xbox One, PC)

The 2016-2017 NBA season is just getting started, but the developers of NBA 2K have been perfecting their league-leading basketball sim for well over 15 years now. Their work has paid off with the best looking, best playing, and flat-out best sports game on the market. An improved Career mode, a deeper MyGM, and countless nips and tucks to the already excellent gameplay leads to another championship year for the basketball dynasty.

Titanfall 2
($60 | PS4, Xbox One, PC)

Squeezed between Battlefield 1 and Call of Duty: Infinite Warfare, this sequel was put in a tough spot on the release calendar. But Titanfall 2 is the sort of game any shooter fan shouldn t miss. It once again delivers fantastic giant mech multiplayer, but this year s model includes one of the most inventive, exciting solo campaigns of 2016, too.

Uncharted 4
($60 | PS4)

Though it came out at the beginning of 2016, Nathan Drake s final adventure (for now) remains a must-have for PS4 owners. Hang on ledges, make precarious leaps, and blast bad guys as you hunt down a legendary pirate treasure. While its gameplay is great, its cinematic delivery is off the charts. This is perhaps the best-looking video game of the year.

Watch Dogs 2
($60 | PS4, Xbox One, PC)

Hackers manipulating real-world events by breaking into supposedly secure online systems? As if that could really happen! Alas, we have video games like the excellent open-world romp Watch Dogs 2 to help us experience such far-fetched fantasies. Set in San Francisco, this sequel improves on the original with a great script, tons of activities, and a wealth of gadgetry that let you stick it to The Man by hacking through an interconnected city.

=~=~=~=

->A-ONE Gaming Online   -   Online Users Growl & Purr!
  """""""""""""""""""

Atari Jaguar Fighting Game Thea Realm Fighters Discovered and Released

It is not all that often that we receive news that a new Atari Jaguar game has been discovered and released. That is exactly what is going on with Thea Realm Fighters though. Thea Realm Fighters is an unreleased one-on-one fighting game for the Atari Jaguar console. For many, this is a Holy Grail of unreleased games as it was only really shown at the 1995 Consumer Electronics Show. As with most unreleased titles, there are multiple versions and only one is available for download at this time.

Thea Realm Fighters was originally developed by High Voltage Software, the company behind Fight for Life (3D fighter) and the port of NBA Jam: Tournament Edition to Atari Jaguar. On an emulator Thea Realm Fighters supposedly runs almost as slow as Fight for Life does on an actual Atari Jaguar console. On actual hardware AtariAge members have reported using various Skunk Boards to play the beta version of the game and stated that it is quite decent in speed. Your mileage may very well vary.

Thea Realm Fighters was in development right around the time that digitized fighting games were still raging on. Even Capcom got in on it with a Street Fighter II: The Movie game that featured digitized actors from the feature length film it didn t work out all that well for them either.

Our friends over on Retrocollect were able to track down the man behind this release and get a quote from him. Mr. Nicholas Persijn told Retrocollect, I m always looking for ways to expand the Atari Jaguar fan scene. [The Realm Fighters] has been a personal holy grail for years and when I finally got my chance, I couldn t keep it for myself.

Allegedly, there were to be 20 fighters featured in Thea Realm Fighters. This is interesting as it would have definitely been a large cast for a period when eight to twelve fighters were common. As you can see in the gameplay video above that the game featured line scrolling floors and fairly colorful backgrounds. This was probably due to the fact that the Atari Jaguar was a color pushing tour de force of a console.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Trump Transition Team Appointments Indicate A Bid To Dismantle Net Neutrality

President-elect Trump has made it clear that he is more than a little hostile towards the FCC s implementation of net neutrality, both in his own words and, today, the appointment of two long-time adversaries of the policy to his transition team.

Jeffrey Eisenach is an economist and government veteran who worked at the FTC in the 80s; he s worked for a number of think tanks and research institutes that transmute industry money into custom expert critique, and under their auspices was a vocal opponent of the FCC s current net neutrality rules. The New York Times did some excellent reporting on the man back in August, if you re curious about the possibility of conflict of interest.

Eisenach described net neutrality as an effort by one set of private interests to enrich itself by using the power of the state to obtain free services from another in his testimony before the Senate Judiciary Committee in 2014. He suggested ISPs have no reason to discriminate between services, and they engender innovation rather than stifle it. You may judge that idea on its own merits.

Mark Jamison worked on Sprint s lobbying team in the 90s, and like Eisenach has done expert consulting work for several organizations. In a recent op-ed, he called net neutrality a growing miscellany of ex ante regulations that frequently work against the entrepreneurs and consumers the rules are intended to help.

He and Eisenach are both scholars at the American Enterprise Institute, a non-partisan think tank (I put that in quotes because while both are in fact actually professors, the term scholar in that context is a bit difficult to pin down). They also both contribute regularly to Tech Policy Daily, a right-leaning tech policy blog composed mainly of grousing at the inefficacy of the current administration and organizations like the FCC.

The FCC itself declined to comment on the appointments or whether they would be working with the Commission in any official way, but even if Eisenbach and Jamison are strictly advisory, they are in a position to exert quite a bit of leverage. How Eisenbach in particular can be considered not to be a lobbyist, however, by an administration ostensibly critical of employing them, is something of a mystery.

With the current congressional makeup and a President-elect hostile to the idea of net neutrality, it s probable that the rules enacted by the FCC have little time left. Republican legislators opposed the FCC rules but faced the prospect of an Obama veto if they attempted to pass a law nullifying them or stripping the FCC of its authority to regulate ISPs as it has. At this point it seems to be only a matter of time before the rules are rolled back.

Net Neutrality, Beloved by Netflix,
Looks Headed for the Ax Under Trump

President-elect Donald Trump shares a specific agenda for his first 100 days in office in a newly uploaded video to his transition team’s Facebook page.
netneutrality

The days could be numbered for Net neutrality under the Trump administration.

Net neutrality rules, passed in February 2015 by the Federal Communications Commission and supported by Netflix, Google and other big websites, prevent Internet service providers (ISPs) from blocking and slowing the transmission of content. The contentious issue triggered lawsuits from the ISPs and drew an unprecedented outpouring of public comments.

Though Net neutrality wasn’t a constant topic for Donald Trump as a candidate, he has been an opponent of the regulations, calling the FCC’s adoption "a power grab" by President Obama in a tweet in 2014.

The president-elect’s latest appointments suggest he’ll try to bolster that view, supported by telecommunication companies such as Verizon and others, by reversing the rules. Jeffrey Eisenach, who joined Trump’s transition team in October, and Mark Jamison, a former lobbyist for Sprint, were named Monday as members of the "Agency Landing" team focusing on the FCC.

Both advisers opposed Net neutrality. Net neutrality "is not about protecting consumers from rapacious Internet service providers. ... Net neutrality is crony capitalism pure and simple   an effort by one group of private interests to enrich itself at the expense of another group by using the power of the state," Eisenach wrote in 2014 in an article on the website of the American Enterprise Institute, a free enterprise think-tank where Eisenach was a visiting scholar from 2012 to 2016.

A recent New York Times article noted that some of Eisenach’s work at the think-tank on FCC issues were supported by Verizon and the GSMA, a wireless trade group of which AT&T and Verizon are members.

Eisenach, who is the managing director and co-chair of communication, media and Internet practice at NERA Economic Consulting, declined comment on the administration’s plans.

Jamison has also taken swings at the Obama administration’s Net neutrality stance. The FCC has pursued a "unilateral approach" on Net neutrality and other rulemaking procedures that "forces industry and consumers to incur unnecessary litigation costs and to operate in an uncertain environment," Jamison said in an editorial last year. Jamison, the director of the Public Utility Research Center at the University of Florida, also declined comment.

The issue of Net neutrality has divided telecom and tech companies for years. Netflix, Google, Twitter and other household tech names back the FCC’s need for authority to prevent ISPs from promoting their own content over that of other outlets.

Telecommunication giants such as AT&T and Verizon have countered, saying the agency used outdated authority given to public utilties that is more heavy-handed than needed to oversee the Internet. Their fight has gone to the courts. Verizon successfully had the FCC’s 2010 rules tossed out in its court challenge in 2014; AT&T and others appealed a federal court’s decision upholding the current rules.

Supporters of a less hands-on FCC see good signs. "l do think the appointment of Eisenach and Jamison is an indication that President-elect Trump is serious about achieving communications policy reform, including curtailing the reach of the agency’s Net neutrality," said Randolph May, president of the Free State Foundation, a free market think-tank.

In a Washington Times editorial Monday, May said "It s undeniable that the Obama administration s FCC has been on a regulatory binge, adopting a number of major overly burdensome and unduly costly new rules, despite the lack of evidence of market failure or consumer harm."

How could Net neutrality be overturned? "The new FCC could try to walk away from the rules. It could refuse to enforce them, try to wipe them off the books or stop defending them on appeal," said Matt Wood, policy director at Free Press, an awareness group that supported the rules.

The strongest action would be congressional, May said, "because it is more durable and can’t be easily reversed." New legislation could remove the FCC’s oversight of the Internet service providers as "common carriers" and the Net itself as a public utility. The FCC based its new rules on authority from Title II of the Communications Act of 1934.

"Republicans in both Congress and the FCC have expressed their antipathy towards Title II regulation," research firm Moffett Nathanson said in a note to investors after the election. "A congressional rollback of Title II was never a serious option in a Democratic administration: President Obama made clear that he stood ready with a veto. With the risk of a veto now gone, a legislative remedy now not only looks possible, but likely."

Analysts Craig Moffett and Michael Nathanson said last week in a subsequent note, "It is likely ... that virtually every major FCC rulemaking of the past four years will be undone."

Net neutrality rules are very popular and drew a record number of comments at the FCC   more than 4 million, said Chris Lewis, vice president at Public Knowledge, a consumer tech advocacy group. Perhaps the Trump administration will offer a counterproposal, he said, because many congressional Republicans were in favor of an open Internet but against the FCC s Net neutrality proposal.

"We think we have very good rules, and we want to defend them," Lewis said, "and if folks want to eliminate these very important consumer protections that are wildly popular across ideological lines, the question is how are they going to protect an open Internet if they eliminate these rules?"

FCC Chairman Tom Wheeler, when asked about possible reversal of the rules after the agency’s monthly meeting last week, said, "I think it’s an important thing to remember that taking a fast fair and open Internet away from the public and from those who use it to offer services to the public would be a real mistake."

Wheeler, a Democrat, noted at the time that serves as chairman at the pleasure of the president, could be replaced. "I am committed to the smooth transition," he said.

Mossberg: Facebook Can And Should Wipe Out Fake News

Totally false news isn t a new thing in the United States. In our fourth presidential election, in 1800, two of our most brilliant founders   John Adams and Thomas Jefferson   faced off in a vicious campaign that involved newspaper editors on the take, and numerous false, often personal attacks. Some historians even claim that partisans for Adams spread the rumor that Jefferson was dead. (He won anyway.)

But they didn t have Facebook to present, amplify, and repeat those falsehoods instantly to millions of people. And that s why the fake news problem is so serious, even outside the context of a presidential election.

Back in May, the Pew Research Center found that roughly 44 percent of the US adult population got at least some of its news from Facebook. And that was before the general election. There s nothing inherently wrong with this. Many if not most news organizations, old and new, big and small (including this one), post stories and videos on the social network. And readers and viewers are moved to share stories, whether publishers have embraced the platform or not.

But that puts a heavy responsibility on Facebook to make sure it s not helping to spread outright lies masquerading as news or publishing the output of made-up news organizations. Yet that s exactly what happened during the 2016 presidential campaign. In the best-known example, BuzzFeed discovered that over 100 mostly pro-Trump fake news sites in a single town in Macedonia were pumping out false news on Facebook in an effort to make money from ads.

Since then, Facebook CEO Mark Zuckerberg has posted two long statements on the social network. On November 12th, while he said, We don’t want any hoaxes on Facebook, he also said it was extremely unlikely hoaxes changed the outcome of this election. But that was a weaselly excuse. Facebook has done controversial experiments to investigate whether the News Feed can affect emotions   surely fake news can affect beliefs as well.

A week later, in the second post, he got more detailed and outlined a series of steps the company was working on. These included better detection of fake news, a better reporting system for users to report fake news, and possibly flagging fake news with warning labels.

"Facebook has done controversial experiments to investigate whether the news feed can affect emotions   surely fake news can affect beliefs as well"

(Oddly, both posts briefly disappeared Tuesday. Shortly after The Verge reported that they were gone, they returned and the company said it was due to a system error.)

In both posts, Zuckerberg stressed the difficulty of deciding what was true or false, what was legitimate opinion or fact, and the need to balance dealing with fake news with protecting freedom of speech.

I agree that these considerations, and others, make this a delicate problem to solve. I especially agree that free speech and the right to opinions, on politics and everything else, must be protected   whether they are popular or not   as long as they aren t hate speech.

But I am also convinced that Facebook has the financial, technical, and human resources to ferret out and totally block almost all fake news and hate speech, both of which it says it wants gone from its service. It s a company that earned nearly $3 billion just last quarter, and which is reportedly building a tool capable of preventing controversial content from appearing in its News Feed in countries like China.

Yet the Zuckerberg posts suggest that, while the company is working to better detect fake news, it s still hoping to rely on the all-too-common Silicon Valley belief that the wisdom of the crowd, plus third-party input, will save the day.

 We do not want to be arbiters of truth ourselves, Zuckerberg says, but instead rely on our community and trusted third parties. Thus, among the ideas he lists for banishing fake news are those labels, that easier user reporting of fake news, and making fake news economically less enticing for its creators. (The company did bar known fake news sites from its ad networks, as did Google.)

"Facebook has the financial, technical, and human resources to ferret out and totally block almost all fake news and hate speech"

But Facebook isn t just a technology platform where news happens to be published, along with baby pictures, vacation bragging and amateur sports commentary. It s clearly a media company. It is now publishing articles and videos directly from a host of news organizations, including The Verge. Including this very column. These are encoded in a special way to work best on Facebook, and there are business terms behind the practice. Increasingly, people read news on Facebook and never even visit the originating site or publication.

Hell, even those Macedonian teens understood that Facebook was a media company. They made up fake media organization names from which to post. (Really, Facebook, you weren t even a little suspicious about DonaldTrumpNews.co?)

So, yes, in my view, Facebook has a direct responsibility to get rid of fake news, and it cannot simply rely on its audience or others to shoulder the burden. I m happy to see tools made available to readers that help report such trash, and happy that Facebook is working with third-party fact checkers. But the ultimate responsibility is Facebook s.

Nobody wants Facebook to tinker with legitimate news and opinion again, except for hate speech. But getting rid of purely fake news from purely fake sources is an eminently achievable task, especially for a well-funded, tech-savvy, huge media company serving nearly 2 billion people.

Here are a few guidelines, Facebook.

Assertions by actual people, even if they are false, aren t fake news. People say and believe all kinds of things. So, even if they don t believe in the moon landings, and form a Facebook group of like-minded others, that s not fake news.

Opinions aren t fake news. The existence of the new MacBook Pro is an indisputable fact, as are its specs, design, and price. Yet some might love it and others might hate it. The same goes for Donald Trump s promise to build a border wall and for the Gilmore Girls revival. But neither the lovers nor the haters are creating fake news.

Differing interpretations aren t fake news. Millions may have seen the video of a football play, from multiple angles. So there s a real, actual fact there. I might think there was pass interference, and somebody else might not, but even if the replay shows there was a proper penalty, the other guy has a right to stick to his guns.

Sensational news stories with little or no reporting that seem opportune, and aren t quickly replicated or even repeated with credit by reputable news sources, are probably fake news. You have the means to investigate this. It might be a new, legit, one-person blog that stumbled onto a great scoop, but it s likelier to be a cash-driven Macedonian teenage fake news poster. How could you not have questioned one of the Macedonian stories that had the Pope endorsing a US presidential candidate? Did you think the Vatican Radio Facebook page would miss that?

Sketchy personal accounts that give every appearance of falsehood and spread fake news (see number 4) were probably established for that very purpose. You know who they are. Humans can often spot them, even if algorithms can t. You can bar them.

I m encouraged that the November 19th Zuckerberg post says the company wants to detect what people will flag as false before they they do it themselves. But, again, I think Facebook needs to step up and take direct responsibility for expunging fake news, not just label it or give it less weight in the news feed.

Facebook might even consider hiring a distinguished, nonpartisan editor and a small staff to help in the effort. The company abandoned such human input in its little-known Trending box after conservatives complained that right-leaning stories were being culled out. But if weeding out verifiably fake news conservative or liberal or whatever   angers some users, that s the price of being a news platform, even if it slightly affects growth. It s the right trade-off.

All of this would mean Facebook would have to act like the media company it has become and stop pretending.

The time for pretending is over.

Facebook Admits That Resisting Standards for Fake News Was ’Wrong’

In the wake of criticism about fake news, Facebook has admitted that its stance of resisting any standards of news on its platform was "wrong."

For so long, we had resisted having standards about whether something s newsworthy because we did not consider ourselves a service that was predominantly for the distribution of news. And that was wrong! Facebook VP of global comms, Elliot Schrage, said on a panel about the election and the media, Vox reported on Friday.

In recent weeks, Facebook has been taken to task for how widely and effectively fake news spread on its platform. A study by BuzzFeed showed that in the lead-up to the election, the top fake-news stories on Facebook outperformed legitimate news stories shared by some of the most popular media companies.

Facebook’s response was initially dismissive, with CEO Mark Zuckerberg saying particularly that "the idea that fake news on Facebook   it’s a very small amount of the content   influenced the election in any way is a pretty crazy idea."

Facebook, however, has recently begun to reevaluate its stance of fake news. Zuckerberg outlined several steps the company is taking to clamp down on the spread of misinformation, and other execs are actively discussing Facebook’s role in the spread of media.

But Facebook has stopped short of pledging to have an editorial role. It is not clear to me that with 1.8 billion people around the world, lots of different users and lots of different languages, the smart strategy is to start hiring editors, Schrage said. That s just not what we do.

In a talk on Thursday, Patrick Walker, a Facebook media partnerships exec, went a bit further. We do not think of ourselves as editors," Walker said during the News Xchange conference in Dublin. "We believe it s essential that Facebook stay out of the business of deciding what issues the world should read about. That s what editors do.

Still, Facebook has admitted that it needs to take some action. We have a responsibility here. I think we recognize that. This has been a learning for us, Schrage said.

EU, U.S. Authorities Take Down Avalanche Global Crimeware Network

After a four year investigation, the Avalanche "crimeware-as-a-service" network was taken down by law enforcement agencies from 30 countries.

Avalanche used as many as 500,000 infected computers daily, and infected millions of computers with malware for harvesting banking and email credentials, according to US-CERT. The crimeware network spread more than two dozen malware families via more than 800,000 domains and provided command and control services for at least eight botnets.

The U.S. Department of Justice and the FBI said in a joint statement, the Avalanche network "is estimated to involve hundreds of thousands of infected computers worldwide. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of dollars worldwide, although exact calculations are difficult due to the high number of malware families present on the network."

The FBI and Justice Department promised more information about the operation would be provided next week.

A press release from the European Police Office (Europol) - the EU’s law enforcement agency, focused on fighting serious international crime and terrorism - said, "The global effort to take down this network involved the crucial support of prosecutors and investigators from 30 countries."

The investigation was started in 2012 by the Public Prosecutor’s Office in the German town of Verden and the Lüneburg Police (Germany), and was carried out with cooperation from the U.S. Attorney’s Office for the Western District of Pennsylvania, the Department of Justice and the FBI, Europol, Eurojust (the EU agency for judicial cooperation on cross-border criminal investigations) and other global partners.

Europol said the law enforcement actions resulted in arrest of five individuals, searches of 37 premises, and seizure of 39 servers. "Victims of malware infections were identified in over 180 countries. Also, 221 servers were put offline through abuse notifications sent to the hosting providers. The operation marks the largest-ever use of sinkholing to combat botnet infrastructures and is unprecedented in its scale, with over

800,000 domains seized, sinkholed or blocked."

"Cyber criminals utilized Avalanche botnet infrastructure to host and distribute a variety of malware variants to victims, including the targeting of over 40 major financial institutions," according to the US-CERT alert on Avalanche. "Victims may have had their sensitive personal information stolen (e.g., user account credentials). Victims’ compromised systems may also have been used to conduct other malicious activity, such as launching denial-of-service attacks or distributing malware variants to other victims’ computers."

In addition, criminals used the Avalanche crimeware infrastructure to operate "money mule" schemes in which people were recruited to commit fraud by transporting or laundering stolen money or merchandise. The money mules accept stolen money or merchandise from a criminal or criminal organization and then forward it, usually after deducting some portion as a "commission," as directed by the criminals; this makes it difficult for investigators to trace the identities of the criminals involved.

According to US-CERT, "Avalanche used fast-flux [Domain Name System (DNS)], a technique to hide the criminal servers, behind a constantly changing network of compromised systems acting as proxies."

Criminals use fast flux DNS techniques, changing DNS records automatically and frequently, to protect against disruption by authorities. Avalanche actually used a "double fast flux network," according to the National Crime Agency (NCA) in the U.K., one of the law enforcement agencies involved in the takedown. NCA stated double fast flux changes IP address records as well as changing the authoritative DNS server for domains, further muddying the waters for investigators.

The Avalanche operation may serve as a model for future international efforts to tamp down cybercrime.

"Avalanche shows that we can only be successful in combating cybercrime when we work closely together, across sectors and across borders," said Julian King, European Commissioner for the Security Union, quoted in the Europol press release. "Cybersecurity and law enforcement authorities need to work hand in hand with the private sector to tackle continuously evolving criminal methods."

"Avalanche has been a highly significant operation involving international law enforcement, prosecutors and industry resources to tackle the global nature of cybercrime," said Rob Wainwright, Europol Director. "The complex trans-national nature of cyber investigations requires international cooperation between public and private organizations at an unprecedented level to successfully impact on top-level cybercriminals. Avalanche has shown that through this cooperation we can collectively make the internet a safer place for our businesses and citizens."

Investigating cybercrimes is often hampered by the difficulty of attribution, Chris Pogue, CISO at Sydney-based cybersecurity company Nuix, told SearchSecurity by email. While the use of anonymity tools like Tor and the use of compromised systems as jump boxes to obfuscate the source of attacks can make it difficult to identify the source of an attack, it’s not impossible.

"The evidence required to satisfy the burden of proof in this regard is significant, and the investigative analysis must be flawless," Pogue said. "Adding to the challenge is the acquisition and execution of a Mutual Legal Assistance Treaty or MLAT, which basically allows foreign law enforcement agencies to collaborate on a case that lies outside the borders of their home country. Based on the countries involved, and the complexities of their legal system, an MLAT can take, on average, anywhere from 10 months to a year (longer in some instances) to successfully process."

The scope and breadth of the investigation - including investigators located in 41 different countries, investigating 16 criminal leaders in 10 different countries - made the Avalanche operation unique. "Understanding the complexity of such a far reaching investigation, and the political and legal challenges that needed to be addressed, the resulting raids and arrests are nothing short of amazing," Pogue said. "This is a tremendous feat by these agencies, and they should be commended for their dedication, tenacity, and commitment to bring to justice those individuals that choose to commit these crimes."

"There’s no denying the fact that this is a major win for the good guys. The Avalanche servers that were taken down in this raid represent a critical piece of criminal infrastructure that was responsible for a sizable portion of the threats we see encountered on the internet each day," Michael Covington, vice president of product at Wandera, the London-based mobile security company, told SearchSecurity by email. "I suspect we will see a measurable drop in global threat encounters over the coming days and weeks. Considering the type of phishing and botnet attacks typically launched through Avalanche, this is particularly good news for consumers during the upcoming holiday season." However, while the takedown may disrupt cybercrime operations it will likely not end them.

"We can expect that someone else will fill the void left by Avalanche, as there is an incredible amount of competition in the criminal underground where crime-as-a-service lives," Ed Cabrera, chief cybersecurity officer for Trend Micro, told SearchSecurity by email. "We can expect another cybercriminal group and infrastructure to take its place in the near future."

Covington said, "We have seen similar takedowns in the past and the criminals always come back with something new and bolder than before. When spam servers were taken down in the 2000s, we saw the rise of distributed botnet services. As C&C infrastructure was interrupted, we started seeing more clever attacks that involved evasive, polymorphic malware."

"Arguably, this is not a race with a clean finish line," Cabrera said. "This is a constant effort for law enforcement, in partnership with the security industry, to identify, investigate and mitigate this threat and the cybercriminal groups behind it."

"What enterprise customers need to realize is that these criminal operations are for-profit entities. An interruption to their network is an interruption to their cash flow," Covington said. "The malicious infrastructure will return and it will morph along the way. They should not become complacent and assume we understand the attacker."

"Crime, like all ecosystems, adapts as circumstances change. All we can really do is reduce the incentives for criminality," John Bambenek, threat systems manager at Fidelis Cybersecurity, told SearchSecurity by email. "In the end, however, we have not solved murder, rape or theft and we won’t likely end cybercrime either."

Check If You Were Hit by the Massive ’Avalanche’ Cybercrime Ring

The U.S. government has posted links for free scanning programs so companies and individuals can check their computers to make sure they weren’t victims of a massive, international cyber criminal operation that was taken down Thursday after a four-year investigation.

 This is probably the biggest operation that law enforcement has ever done against cyber crime, said Catalin Cosoi, chief security strategist with BitDefender, one of the dozens of companies worldwide that worked with law enforcement to attack the group.

The U.S. Computer Emergency Readiness Team has posted links to five scanners on its site. Europol has also posted a list of sites in multiple languages for potentially infected users.

Known as "Avalanche," the group had been active since 2009, according to the FBI and Europol, the European law enforcement agency. It was effectively a criminal company that sold and rented cloud-hosted software to other criminals who used it to take over systems, infect networks, launch ransomware or create enormous robot networks (botnets) to send spam.

Avalanche networks were also used to launch targeted attacks against banks and to recruit people to illegally transfer stolen money between countries, known as money mules.

"They sent more than one million e-mails with damaging attachments or links every week to unsuspecting victims," and involved as many as 500,000 infected computers worldwide on a daily basis, Europol said in a release.

 They would do whatever you wanted. You just had to call them, say I need command and control service, or I need to infect this type of people or this type of business, and they d do it, said Cosoi.

The investigation originally began in Germany in 2012 after prosecutors there detected a ransomware operation that blocked access to a substantial number of computer systems and allowed the criminals to do bank transfers from the victims’ accounts.

As authorities became aware of the scope and reach of the criminal organization, the effort to shut it down ended up involving prosecutors and investigators in 30 countries.

On Wednesday, law enforcement launched a concerted action against the Avalanche group. It resulted in five arrests, the search of 37 premises and seizure of 39 servers. In addition, over 800,000 Internet domains, or addresses, were seized to block the criminals access to their customers.

Now that the operation has been taken down, the next crucial stage is for infected individuals and companies to check to make sure that their computers do not have Avalanche malware on them.

 Companies and consumers should take this opportunity to scan their systems for the different families of malware that the Avalanche botnet distributed, said ESET senior security researcher, Stephen Cobb.

Multiple companies worldwide have written tools to run this scan.

As Europol said on its website, "computer users should note that this law enforcement action will NOT clean malware off any infected computers   it will merely deny the Avalanche users ability to communicate with infected victims computers. Avalanche victims computers will still be infected, but shielded from criminal control."

While the effort was hailed in the cyber security world as a major coup against cyber crime, the differential between how fast international cybercrime networks proliferate and how quickly international law enforcement can act is troubling.

 It does give some reason for concern that our anti-cybercrime efforts still can’t match the speed and dexterity that cyber criminals use for their own efforts," said Nathan Wenzler, principal security architect at AsTech Consulting, a San Francisco-based security consulting company.

Unfortunately, while he believes that dismantling the Avalanche network will certainly show some short-term gains, he expects the cyber criminals will be "back up and running in short order.

Enigma Codebreaking Site To Become Elite UK Cyber Defense School

Bletchley Park, where British codebreakers famously cracked Nazi Germany’s Enigma cypher, is to become home to the country’s future cyber defenders. An elite school for talented teen hackers is planned for the site, to open in 2018.

During World War II the mansion house in Buckinghamshire, England, was home to the British government’s Code and Cypher School, whose critical but top secret work has become well known through books and movies like the Oscar-winning "The Imitation Game."

The school, with capacity for up to 500 students ages 16 to 19, is part of a plan to strengthen the UK’s defenses against what experts say are growing cyber threats.

Alastair MacWillson, chair of Qufaro, the cybersecurity group behind the project, said he expects the site’s distinguished history to be an inspiration to students.

"It’s a rich story. We’re leveraging the legacy and heritage," he said. "The government says cyber security and the measures to defend the country are the new codes and cyphers. So where better to do this?"

MacWillson said the initiative will harness the expertise in Britain’s young hacker community and put them on a pathway to safeguarding the country’s cyber security.

"There is some real talent out there, people with extraordinary capabilities in this area, and its usually youngsters that are good at gaming theory and hacking systems," he said.

However, while there are centers of excellence for this specialization at the university level, gaps in the education system currently allow talent to slip through the cracks at the high school level, MacWillson said.

"The government was concerned on two fronts - that the country isn’t capturing raw talent, but also that it’s maybe letting raw talent err onto the dark side," he said.

The school will be a so-called "genius college" for prodigiously talented students, with 40% of the curriculum devoted to cyber learning and the rest to STEM subjects such as math and engineering.

The school would also take advantage of an existing incubator for tech companies based at Bletchley Park to provide internships for students.

People drafted in as codebreakers were often found by tests requiring them to complete The Daily Telegraph&#39;s crossword in under 12 minutes.

All workers at the estate were ordered to sign the Official Secrets Act. For many young girls at the park, this meant that their families had no idea where their 18-year-old daughters had been sent.

Her Majesty the Queen visited Bletchley Park in 2011, and received an Enigma machine demonstration from Ruth. The monarch called the contraption &quot;splendid.&quot;

Britain’s Government Communications Headquarters (GCHQ), as the former Government Code and Cypher School is now known, has applauded the plan, saying it "welcomes initiatives that promote and develop skills in cyber security."

A GCHQ spokeswoman said the concept was "interesting, especially if it can provide a pathway for talented students from schools that are not able to provide the support they need."

The head of MI5, Britain’s security and counterintelligence agency, warned last month that the country faced a growing covert threat from Russia, involving "high-volume activity out of sight with the cyber-threat."

The Kremlin rejected the claims.

Earlier this month the British government unveiled its National Cyber Security Strategy, aimed at tackling cyber threats facing the country and making the UK one of the safest places in the world to do business online.

The UK Now Wields Unprecedented Surveillance Powers   Here s What It Means

The UK is about to become one of the world s foremost surveillance states, allowing its police and intelligence agencies to spy on its own people to a degree that is unprecedented for a democracy. The UN s privacy chief has called the situation "worse than scary." Edward Snowden says it s simply "the most extreme surveillance in the history of western democracy."

The legislation in question is called the Investigatory Powers Bill. It s been cleared by politicians and granted royal assent on November 29th   officially becoming law. The bill will legalize the UK s global surveillance program, which scoops up communications data from around the world, but it will also introduce new domestic powers, including a government database that stores the web history of every citizen in the country. UK spies will be empowered to hack individuals, internet infrastructure, and even whole towns   if the government deems it necessary.

Although the UK s opposition Labour Party originally put forward strong objections to the bill, these never turned into real opposition. The combination of a civil war between different factions in Labour and the UK s shock decision to leave the European Union means the bill was never given politicians   or the country s   full attention. Instead, it will likely inspire similar surveillance laws in other countries. After all, if the UK can do it, why shouldn t everyone else? And there will be no moderating influence from the US, where the country s mostly intact surveillance apparatus will soon be handed over to president-elect Donald Trump.

With this global tide of surveillance rising, it s worth taking a closer look at what exactly is happening in the UK. Here s our overview of what the Investigatory Powers Bill entails:

The UK government will keep a record of every website every citizen visits for up to a year, with this information also including the apps they use on their phone, and the metadata of their calls. This information is known as internet connection records, or ICRs, and won t include the exact URL of each site someone visits, but the base domain. For this particular webpage, for example, the government would know you went to www.theverge.com, the time you visited, how long you stayed, your IP address, and some information about your computer   but no individual pages.

Each Internet Service Provider (ISP) and mobile carrier in the UK will have to store this data, which the government will pay them to do. Police officers will then be able to access a central search engine known as the "request filter" to retrieve this information. Exactly how this request filter will work still isn t clear (will you be able to find every visitor to a certain website, for example, then filter that down to specific weeks or days?), but it will be easy to tie browsing data to individuals. If you sign a contract for your phone, for example, that can be linked to your web history.

There are a few ways this data could be muddied. For a start, services like VPNs and Tor, that bounce your internet traffic around the world, will be difficult to follow. And when it comes to tracking activity on your phone   for an app like Facebook Messenger, for example   this information will be fairly useless, as most of these apps maintain regular connections to the internet throughout the day. "The government won t be able to get all of the data all of the time," Jim Killock, executive director of the UK s Open Rights Group tells The Verge. "But they re not expecting most people to bother to protect their privacy."

The key point about this power, though, is that it has no judicial oversight. Access to citizens web history will be solely at the discretion of the police, with a specially trained supervising officer approving or denying requests. "It makes this kind of surveillance a simple, routine activity," says Killock, adding that without oversight, it ll be impossible to know when police target specific groups disproportionately. That s definitely a problem in a country where even senior law enforcement officers admit that claims that the police force is institutionally racist have "some justification."

Although this power sounds almost farcical in its reach ("The police will know what porn you look at! They ll know how much time you waste on Facebook!"), it s no laughing matter. It s not as intrusive as other measures, but it establishes a dangerous new norm, where surveillance of all citizens online activity is seen as the baseline for a peaceful society. Collect evidence first, the government is saying, and find the criminals later. The country has a surprising tolerance for this, embracing the use of surveillance cameras more than most. Now, though, it has CCTV for the nation s online life.

Other parts of the bill don t introduce new powers, but establish surveillance and hacking activities revealed by the Snowden revelations. These include the collection of metadata from around the world, and targeted hacking of individuals’ computers   bugging their phone calls, reading texts, and so on. Unlike access to browser history, these latter powers will require a warrant from both the Secretary of State and a panel of judges.

The government has given hacking the deceptively understated description of "equipment interference," and splits it into two camps: targeted and bulk. Targeted equipment interference allows law enforcement and security agencies to hack specific devices, phones or computers, while bulk hacking can cover larger groups. The only difference between the two powers is that bulk hacking is only authorized for foreign targets.

We already know quite a bit about these capabilities thanks to Snowden s leaks, and they cover the sort of malware and spyware you might expect any hacker to use. GCHQ s toolkit, for example, includes a collection of programs named after smurfs: "Nosey Smurf" activates a device s microphone to record conversations; "Tracker Smurf" hijacks its GPS to track location in real time; while "Dreamy Smurf" allows a phone that appears to be off to secretly turn itself on.

Out of all the new legislation, targeted hacking has probably been objected to the least. This is because it will require a warrant approved by both government ministers and a specially appointed panel of seven judicial commissioners   the so-called double lock procedure   and will be reserved for "serious crimes" and threats to national security. This sort of interception also takes place on a much smaller scale. The UK police made more than half a million requests for metadata last year, but there were only around 2,700 warrants for directly intercepting communications in the same period.

However, what is new is the authorization of "bulk equipment interference" or the hacking of large groups of people. This power will be limited to the security agencies and can only be used outside of the UK, but the government is clear about its potential scope. It s said that if it needs to hack every phone and laptop in a "major town" to stop a terrorist attack, it will; and it s suggested that it might be used to take over the entire internal email system of a "hypothetical totalitarian state," if it s developing biological weapons.

There s also the worry that the targeted hacking laws could be used to hack multiple people under the use of something called a "thematic warrant." Ross Anderson, a professor of security engineering at Cambridge University who gave testimony about the IP bill to the government, gives the example of the police chief of a UK city wanting to stem knife crime, and asking the government to force Google to get data from Android smartphones. "The point is that it s possible," Anderson tells The Verge. "Perhaps the government has given some private assurances to these companies [that it won t happen], but we know from long experience that such private assurances are not worth the paper they re not written on."

In addition to bulk hacking, the IP bill legalizes the bulk collection of communication data from around the world, activity that Snowden first revealed in 2013. The UK courts judged that this activity was in breach of human rights law earlier this year, but once the IP bill passes, it ll be absolutely legal. Although the government claims that this sort of information is treated respectfully, its own internal memos have shown staff abusing their powers; using bulk datasets for things like finding addresses to send birthday cards, and "checking details of family members for personal convenience."

One of the biggest trouble spots for the bill, though, isn t so much an explicit power as an assumption by the government namely, that it can force tech companies to decrypt user data on demand.

Now, there are a lot of caveats to this statement. Firstly, requests for this data will be on a small scale, like targeted hacking. Secondly, the wording of the bill is ambiguous. It doesn t explicitly force companies to install backdoors in their products, but it does say they should be able to remove encryption on users data whenever "practicable." What exactly "practicable" means is never explained. The UK might argue that it s "practicable" for a company to undermine its own encryption; that company might respond that doing so would endanger its business around the world.

Earlier this year, big tech companies including Facebook, Microsoft, and Google lined up to denounce this part of the legislation. Apple CEO Tim Cook was particularly critical, noting that the law would have "dire consequences" if introduced. "If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It s the good people," said Cook in 2015. "The other people know where to go."

What exactly will happen if the UK government demands that a company like Apple decrypt its data isn t clear. However, it won t be straightforward replay of San Bernardino, when Apple battled the FBI over the decryption of a terrorist’s iPhone. The UK has the legal authority to penalize companies that don t comply, but experts aren t sure whether they would bother. "A lot of this is about setting a precedent of how you think things ought to function, rather than necessarily expecting to be able to enforce the laws against overseas companies," says Killock. In many cases, he suggests, the issue will come down to leverage. Tech companies without any UK presence will be able to shrug off demands (what s the government going to do to them?), but big firms like Apple and Facebook, which have thousands of staff in the UK, may feel more at risk. Alternatively, this might give them an advantage against the government; allowing them to threaten to withdraw jobs, for example.

Experts say what is even more dangerous, is the fact that any such battles between tech companies and the UK government will take place in private. Any warrants issued to a company to decrypt users data will come with a gagging order, forbidding the firm from discussing it. "There wouldn t be any public debate about it," Harmit Kambo, campaigns director at Privacy International, tells The Verge. "Apple vs. the FBI just wouldn t happen in the UK." The first we might know of a battle over encryption could be a company simply withdrawing its services from the UK. "The invisibility of it is the biggest trick they ve pulled," says Kambo. "It s sad that the Snowden revelations backfired so spectacularly here. Rather than rolling back powers, they ve been used to legitimize these practices."

The scope of the law reaches far beyond the UK’s borders, and the knock-on effects will likely be felt in countries around the world. Taken as a whole, it’s hard to see the Investigatory Powers Bill as anything other than a reshaping of the concept of private civil society.

Facebook Is Unlikely To Succeed in China, Even If It Compromises on Free Speech

Facebook may have laid some of the early groundwork to launch its social network in China, but the U.S. company s chances of making a dent in the world s most populous country remain remote.

A New York Times report that Facebook is developing a system that could censor information to appease the Chinese government is the talk of the tech industry right. The timing couldn t be worse: domestically, Facebook is under pressure for failing to adequately manage the influence of fake news on the U.S. election, yet here it is seemingly prepared to quash legitimate information on user timelines to kowtow to the Chinese government and further its interests in a country of 1.3 billion people.

Facebook s China conundrum hasn t changed much since its IPO in 2012, when it admitted it may not ever find a way into the country.

Recently, however, CEO Mark Zuckerberg reportedly justified the development of censorship software, telling staff that it s better for Facebook to be a part of enabling conversation, even if it s not yet the full conversation. That triggered a number of departures, according to the New York Times, but the truth about China is that it would take a huge effort from Facebook to be relevant to the general conversation in the first place.

Even if Zuckerberg   who has made little effort to hide his interest in doing business in China   sold out and agreed to censorship in exchange for being unblocked, Facebook has a major challenge in finding a place to sit within the nation s already-developed social media ecosystem.

Sticking to its roots won t cut it because Facebook-style social networking has already failed in China.

Renren, the company widely labeled as China s Facebook, has long since pivoted. Initial promise saw Renren attract investment from SoftBank in its early days, and before its U.S. IPO in April 2011, the company claimed 160 million users.

That NYSE listing raised $743 million, but the share price has fallen from a first-day close of $18.01 to just $1.81 today. These days Renren s service is barely used and the company is more notable for its investment deals, which include stakes in a mortgage lender and a delivery service. That investment business and its social video platform are being spun out of the company to give them room to breathe, such is the decline of the core service and traditional social networks in China.

Renren and lesser rivals like Kaixin withered because they missed mobile, hugely popular messaging app WeChat didn t and now it is king.

WeChat s dominance has been clear for a long while   I wrote as much back in 2013   and today it has 846 million monthly active users, the majority of whom are in China. It is also a critical part of parent firm Tencent s mobile monetization strategy. More to the point, for Facebook, is that it occupies the space that Facebook is aiming for in China   and then some.

Messaging apps have taken a huge bite into social networks, no where more so than China where you frequently notice people out and about in public using WeChat groups, or holding their phone to their face to use the push-to-talk walkie talkie feature to communicate.

But WeChat goes beyond messaging. It is the internet, and more.

It includes a Facebook-style timeline feed from friends   Moments   consumers can connect with branded accounts as they do with Facebook Pages, there s a payment system, shopping, banking, appointments and now a new feature that enables developers to build their own apps for the messaging platform, thereby disintermediating official app stores.

WeChat is essentially the mobile portal for Chinese consumers, as A16z partner Connie Chan put it, while Twitter-like Weibo covers social with 297 million MAUs, so it is hard to see what new tricks Facebook can bring to the party

Then there s the fact that, in China, your Western brand means very little.

Just ask Uber CEO Travis Kalanick, who agreed to sell his company s China business to rival Didi. Facebook s global appeal is muted in China. Apple and the iPhone are thriving in China as exceptions to the norm, but Facebook doesn t have that same brand gravitas.

The average person in China has no immediate need for Facebook. Sure, you can connect with people who are overseas but, at this point, people who would find Facebook useful to connect with friends or family overseas almost certainly already use it via a VPN. Facebook s ad buying service estimates that the social network has an audience of around 2.1 million users in China, a tiny portion of the country s reported 710 million internet users.

Zuckerberg s burning desire for China seems to be the catalyst for the development of the censorship tool, which the Times report stressed may not ever be deployed, but Facebook should tread very carefully here. Compromising on free speech can only lose it friends in the West, and the chances of any kind of success in China are very slim, which by extension could negatively impact its stock price.

Sticking to its existing strategy of serving advertising customers in China that want to reach a global audience is a better bet but, even then, working with state-run publications as Facebook does   throws up plenty of issues around media manipulation and fake news.

Google Chrome Now Defaults to HTML5 for Most Sites

Google proposed making HTML5 the default over Flash in its Chrome browser back in May. With the latest release, Chrome 55, the company has nearly completed the transition. Chrome now defaults to HTML5 except when a site is Flash-only or if its one of the top 10 sites on the web. For every other website you visit, you’ll be asked to enable Flash the first time you go there.

HTML5 by default has been a long time coming for the browser. Two versions ago, Google began blocking Flash that was running "behind the scenes." The continued change over to HTML5 should lead to faster load times, better security and improved overall performance. The update to version 55 also includes CSS automatic hyphenation that will help with the look of text blocks and line wrapping.

For Android users, the new version brings wider availability of a downloads feature that enables offline viewing of web pages, images and videos. The mobile update is said to be on its way soon, but Chrome 55 is rolling out now to Mac, Windows and Linux users on desktop.

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.